IOSR Journal of Business and Management (IOSR-JBM)
e-ISSN: 2278-487X, p-ISSN: 2319-7668. Volume 20, Issue 3. Ver. 2 (March. 2018), PP 0106
www.iosrjournals.org

Electronic Medical Record for Deliverance of Effective Healthcare Delivery: Ethical Issues and Challenges of Digitalization in Clinical Information and Electronic Medical Records (EMR) Management

*Sakhi John, Assistant Professor ** Dr. N .Ravichandran, Associate Professor , ***Dr. Mohd. Faisal Khan,
Assistant Professor, Department of Health and Hospital Management, School of Management and Business Studies, JamiaHamdard, New Delhi
Corresponding Author: Sakhi John,

Abstract :*There is no denying fact that the application of ethics in medical / health sector have much more significance. In healthcare sector, than any other sector because of many factors which is related to privacy, confidentiality and personal information involved with this sector.No one doubt about Electronic Medical Records have potential to improve clinical care, but this paper focus on mainly the ethical issues of electronic health record in public health sector. Even after the growth of computer technology in medicine and allied subjects, most medical prescriptions and recordings are still documented on paper medical records. We have enormous benefits and advantages for keeping the electronic medical record documentation still EMR's are not very popular because of this issue connected with ethical, legal, confidentiality, security.In current scenario the implementation, development and percentage of utilization of Electronic Health Record is comparatively with other sector is very low. Here in this paper we mainly focused on ethical issues related to facility based integrated record which can share, access, available in public domain.*

Keyword : *Electronic Health Record, Confidentiality, Ethics, privacy*

Date of Submission: 22-02-2018 Date of acceptance: 05-03-2018

I. Introduction

Doctor-patient relationship is the corner stone medical practice. It is a very sacred one as it has evolved through the ages. In the early ages, doctor was considered to be equivalent to God and whatever the doctor said was considered by patients as law and was indisputable. At that time, most of the medical practitioners never charged anything from the patients but lived on thevoluntary offerings made by them. This relationship continued for ages. In modern times, when doctors started charging for their professional advice, it transformed doctor- patient relationship. Now, the patients have started evaluating the professional advice with the money they paid. This evaluation has given new morning to the relationship and has made it more responsive on behalf of medical practitioners.

Right of information

The patient has the absolute right to know about the disease he is suffering from, how thediagnosis is going to be made, how the treatment is planned, what type of anaesthesia is to begiven, what are the choices of treatment available, what are the risks involved if there is anyalternative treatment available and lastly, prognosis and cost of the treatment.

Right of privacy

The patient enjoys the same right of privacy as are available to other people. Whileexamining, the doctor should note that no outsider/ undesirable persons are present duringexamination/treatment. Special care should be taken while examining female patients. It isbetter that examination of female patients may be done in the presence of a nurse or theattendant of the patient.

Right of confidentiality

All the information arising out of treatment of the patient should be kept confidential andshould not be made public without the written consent of the patient.

Right of pictures/video recording

Any picture or video-recording of the patient while receiving treatment should be taken onlyafter the permission of the patient in writing. Even after permission, the identity of the individualshould be kept secret and should not be revealed by pictures or text accompanying them.

Right to change doctor at any stage of treatment

The patient can change his doctor at any stage of the treatment without giving any reason.But in this case the fixing of the responsibility for sharing provider owned electronic record or institution owned electronic health record most difficult part. We need to bind it with strict protocols and regulations for sharing

Legal Aspects of Medical Records

From the time immemorial, importance of medical records is established. For centuries,courts of entire world are relying on medical records in cases of assaults on human body. Themedical record depicts who the patient is, what he is suffering from and why he is suffering.It tells the tales of patient care in hospital.Medical records are both medical and legal records. Medically, it gives a summary ofchronology of illness for patient and reference for other physicians. Legally, they arerequired for courts/insurance companies for settlement of disputes. Despite of changes in the health IT, our courts of law have not widely accepting the electronic signature and electronic handwriting with health record.

As of today, the doctor-patient relationship is a contractual one under the contract act and it establishes immediately once the patient steps into the clinic of the doctor and he agrees to treat him. As we understand that the relationship is contractual and mutually binding, we have to understand the rights and obligations of the doctor and the patient.

Provide answers to important research questions.

The right of the research subject to protect one's integrity must always be respected. Every precaution should be taken to respect the privacy of the subject and to minimize the impact of the study on the subject's physician and mental integrity and on the personality of the subject.There is lot of potential Electronic Medical Records have to improve clinical care. Doctors can access health records through a secure Internet connection at any time.

Enhances coordination of care/ Personalized Healthcare

Electronic health records are more concentrating on personalized healthcare, in the same time its conflicts among several ethical principles of healthcare sector. Electronic Health Records may represent beneficiaries because they are alleged to increase in access to healthcare by individuals, doctors and other para medical staff for their personalized or individualized medical care.

Electronic prescribing has been shown to reduce medication errors.

There is a study that nearly one lakh patient's death occurring in US per year due to lack of accessibility of their information at right time. Aim of the reducing error in healthcare services is to encourage interacting on effect of the reforms and services being compared not simply produce a 'Progress Card' or 'Report Card'. In the U.S., medical errors are estimated to result in 44,000 to 98,000 unnecessary deaths, in hospital settings, and 1,000,000 excess injuries each year.

(There are no figuresaccessible from Indian Healthcare sector; the figures will be much higher than this) A moderate average of both the Institute Of Medicine and HealthGrades reports signifies that there have been between 400,000-1.2 million error-induced deaths during 1996–2006 in the United States. Medical error is a preventable adverse effect care, whether or not it is evident or harmful to the patient. This might include an inaccurate or incomplete diagnosis or treatment of a disease, injury, infection or other ailment. Studies always were based on administrative records, not clinical records, and mainly unseen multi-causality of outcomes. In the U.S., medical errors are estimated to result in 44,000 to 98,000 unnecessary deaths, in hospital settings, and 1,000,000 excess injuries each year.In US the $19.5 billion in total costs, approximately $17 billion was the result of providing inpatient, outpatient and prescription drug services to individuals who were affected by medical errors."

Medical errors are related with inexpert physicians and nurses, new procedures, extremes of age and urgent care. Poor communication whether in one's own language or may be the case for medical tourists in other language, illegible handwriting, improper documentation, inadequate nurse-to-patient ratios, and alike named medications are also known to contribute to the problem. Patient activities may also contribute extensively to medical errors. Falls, for example, are often due to patients' own misjudgement.

Impact Of Implementation Of EMR – Example From Public Health Care System From Delhi (Data Collected From One Public Sector Hospital From NCR After Year Of Installation Of EMR.

	No Change	Much Better
Improved ability to make good patient care decisions due to access to information?	44 (40%	66 (60%)
The accuracy and validity of the patient care data being recorded	40 (36.3%)	70 (63.7%)
The overall safety of patient care	30 (27.2%)	80(72.8%)
The amount of professional satisfaction I get out of my job	45 (40.9)	65(59.1%)
My ability to learn about and improve our patient care processes	50 (45.5)	60 (54.5)
Communications when patients are transferred to other facilities	30(27.2%)	80 (72.8)
Improved ability to make good patient care decisions due to access to information?	44 (40	66 (60.0%)
The accuracy and validity of the patient care data being recorded?	40 (36.4	70(63.3%)
The overall safety of patient care	30 (27,2%	80 (72.8%)
The efficiency of our work processes	45 (40.9%	65 (59.1%
The timeliness with which patient related data can be available	40 (36.4)	70 (63.3)
The timeliness with which patient related data can be available	40(36.4%)	70 (63.3%)
Communications when patients are transferred to other facilities	30 (27.2%)	80 (72.8%
The amount time I can spend directly with patients	30(27.2%)	80 (72.8%)
Legibility and clarity of patient care orders	40(36.4%)	70(63.3%)

Ethical concerns about the EMR

Patients concerns about who has access to their identifiable health information.

Medical Ethics may be defined as a code of conduct accepted voluntarily by medical practitioner within the professional. Legally they are not enforceable by law but are defended by the State Medical Council. Medical ethics have evolved through the centuries. Some of the ethics have evolved into present law. So both the terms, medical ethics and medical law, are synonymous.

While cyber criminals are a growing threat as seen by the recent ransomware debacles, it can't be the only area of focus to protect EHR. In the recent *2016 State of Data Security and Compliance Report* published by Ipswitch, Inc, more than 500 IT professionals (91 in healthcare organizations) from around the world were surveyed about their data security policies. Those in healthcare organizations that identified as having experienced a significant data loss noted that only 20 percent was due to malicious activities, while 45 percent was due to human error and 35 percent due to process or network failure. Interestingly, in that same report only 34 percent in healthcare reported their organization as very efficient in identifying risks and 42 percent as very efficient in mitigating risks.

Another issue

There's a perfect storm of events that are causing an increase in cybercrime: national laws and policies have encouraged healthcare organizations to move to EHR (98 percent of hospitals in US); available technology to ease the transition to EHR; and high value for EHR on the black market (FBI Cyber Division Private Industry Notification #140408-009, 8 Apr. 2014, puts the value at $50 for each partial EHR).

Confidentiality of the identifiable health information in the EMR

All medical records are confidential. One cannot release them without the permission thepatient or his authorized representation patient can give permission to release and better totake it in a written form. If a patient has died his next of kin or authorized representative cangive consent for release documents.

A single electronic breach could affect more patients than a breach of confidentiality with paper records.

There are number of examples available for In Ohio, a medical school health centre mistakenly posted online treatment information, names, and addresses of 2,800 patients.In Florida, the names of 6,000 persons with HIV infection were mistakenly attached to an email sent to 800 employees in the county health department

Code of medical ethics

The oldest code of medical ethics is the Hippocratic Oath. Even after twenty five centuries.

International code of medical ethics

A doctor must always retain the highest standards of professional conduct and must practice his/her profession uninfluenced by intention of profit.The following practices are deemed unethical such as:

Any self advertisement except such as is clearly authorized by the national code of medical ethics. Association in any form of medical service in which the doctor does not haveprofessional independence.

Remedies to enhance the security of electronic records andPreventing Hacks for Safeguarding Patients

1. Passwords
2. Timed logouts.
3. Restricted access, encryption, and secure websites
4. The need for strong security measures is very evident and it is equally clear that action needs to be taken right away. Some of the best practices to implement to advance security and limit harm during breaches are:
5. Educating the hospital's top management about the impact of poor security and its consequences on patient retention. The education mustincorporate creating awareness about using strong passwords at all entry points to make it difficult for outsiders to simply get access by guessing the correct combination of letters/ characters.
6. Assessment of hospital's firewalls and security measures with evaluation of security levels of third party networks to which the hospital's network is linked.
7. Making equipment on the network difficult to identify so that hackers cannot quickly hone in on highly vulnerable machines/ equipment to cause a disruptive attack.
8. Establishing a security breach response team that can quickly act when a breach is detected so that the damage can be minimized.

A Washington Post news report in August this year came as a shock to many Americans who believed, until then, that their medical records were for their eyes only. Chinese hackers stole data pertaining to a massive 4.5 million patients from a company that runs over 200 hospitals spread across the US. The massive data breach raised some grave concerns about how private medical records are and exactly what various health care organizations are doing to keep this sensitive information completely confidential like it ought to be.

In fact, the first question in the mind of every patient comeswho has ever paid a visit to their physician is that: Is my hospital doing anything at all to safeguard my privacy

Using the EMR for advertising

A large chain of pharmacy outlets and a drug manufacturer formed a partnership to identify patients who might benefit from a new drug.[4]To advertise this more convenient dosage, the manufacturers used the pharmacy chain's electronic records to identify patients who had received prescriptions for antidepressantsMany recipients of the mailing were outraged and many were angry that sensitive information about their psychiatric condition had been accessed without their knowledge or permission

This episode reveals the discrepancy between clinical and business views of the confidentiality of personally-identified health information.

Using the EMR for outcomes research

There are also ethical concerns about using the EMR for outcomes research. Although there is no physical risk to patients, there are psychosocial risks. Patients may be harmed if confidentiality of their personal health information is breached. In the era of digitalization and computers allows healthcare information to be used in innovative ways that offer important benefits to patients and to the public. At the same time, such access to identifiable health information raises ethical concerns, particularly concerns about confidentiality.

HIPAA/HITECH identifies IT controls to protect data including encryption, network perimeter defence, effective access control and employee training, and yet data loss is a growing trend

According to the records reviewed by NBC News, medical records of at least 7,000 people compromised in a data breach involving Bronx Lebanon Hospital Centre in New York disclosed patients' mental health and medical diagnoses, HIV statuses and sexual assault cases and domestic violence reports.

Other information in the compromised records, which online security experts said spanned 2014 to 2017, included names, home addresses, addiction histories and religious affiliations.

From many years the healthcare industry has been a main target for cybercriminals. Here is a sum up of the biggest data violation from healthcare companies.

In the past five years, we've seen healthcare data breaches grow in both size and frequency, with the largest breaches impacting as many as 80 million people. Healthcare data violations expose highly sensitive information, from personally identifiable information such as Social Security numbers, names, and addresses to sensitive health data such as Medicaid ID numbers, health insurance information, and patients' medical histories.

The motives behind cyber attacks on healthcare companies are clear: hospitals, urgent care clinics, pharmacies, health insurance companies, and other healthcare providers keep records of very valuable information – more "juicy details" that can be used for identity theft than almost any other industry. What's more, the healthcare industry is widely regarded as having rather weak security; a recent report from SecurityScorecard ranks healthcare 9th out of all industries in terms of overall security rating.

This is not a small problem. A February 2017 survey from Accenture reveals that healthcare data violations have affected 26% of U.S. consumers, or more than one in every four Americans. In addition, the survey also found that 50% of breach victims in the end suffered medical identity theft, with an average of $2,500 out-of-pocket costs. Even in extreme of cases, half of the survey respondents reported that they learned of the breach themselves as opposed to an official company or law enforcement notification after they had been alerted to an error on their benefits explanation, credit card statement, or similar documents.

These are facts especially when you consider the broad reach of the healthcare industry and within the healthcare systemalmost everyone has healthcare records.

Below are the top 10 biggest healthcare data violations, according to the U.S. Department of Health and Human Services Office for Civil Rights (listed by size, from the smallest to the largest in terms of the number of individuals affected):

10. NewKirk Products: 3.47 Million Affected (August 2016)

In mid-2016, healthcare ID card-issuer NewKirk Products announced a data breach that victimized an estimated 3.47 million patients. Among those impacted were several branches of the insurer Blue Cross Blue Shield, which is one of the largest health insurance providers by enrolment in the United States. Hackers reportedly gained access not only to primary care provider information, but also to sensitive personal information including Medicaid ID numbers, names (including those of dependents), and dates of birth, premium invoice information, and group ID numbers.

9. Banner Health: 3.62 Million Affected (August 2016)

Again in mid-2016, Banner Health, an Arizona-based healthcare provider, disclosed a cyber attack that had compromised the records of 3.62 million patients. The discovery came after staff detected unfamiliar activity on Banner's private servers. Then Banner hired a cybersecurity firm to examine and discovered two attacks in which hackers accessed patient records and payment systems data. Compromised data may have included names, credit card numbers, expiration dates,internal verification codes, addresses, birth dates, Social Security numbers, doctors' names, and healthcare information.

8. Medical Informatics Engineering: 3.9 Million Affected (July 2015)

In mid-2015 a banner year for healthcare data violations – A Medical Informatics Engineering company that creates electronic medical records software, announced a data breach that affected at least 11 healthcare providers and 3.9 million patients. Affected patients received a notice in the mail that their personal information such as names, phone numbers, mailing addresses, dates of birth, diagnoses, Social Security numbersand other sensitive information had been filched.

7. Advocate Health Care: 4.03 Million Affected (August 2013)

In mid-2013, Advocate Health Care revealed several data breaches including two computer theft which revealed personal information and unencrypted medical records of 4.03 million patients. News of the massive breach came just four years after the company reported a theft of unencrypted data; encryption protocols were passed after that 2009 incident, but had not yet been arranged at the offices affected in 2013. In August 2016, Advocate agreed to pay $5.55 million to settle a lawsuit related to the violation.

6. Community Health Systems: 4.5 Million Affected (April-June 2014)

In mid-2014, Community Health Systems, which operates 200+ hospitals throughout the U.S., announced a major healthcare breach that affected 4.5 million patients. Attackers exploited a software vulnerability to access

Social Security numbers, dates of birth, phone numbers, and physical addresses. The breach affected anyone who had received treatment at one of CHS's network-owned hospitals in the past five years as well as any individuals who had been referred to CHS by an outside doctor during that period.

5. University of California, Los Angeles Health: 4.5 Million (July 2015)

The UCLA Health System was another healthcare organization to reveal a data violation in 2015. In mid-year, the university's Health System announced that hackers had accessed the records of 4.5 million patients.UCLA admitted it hadn't encoded its patient data with an admission that drew harsh censure from security experts.

4. TRICARE: 4.9 Million Affected (September 2011)

In late 2011, Science Applications International Corporation (SAIC) announced a data violation that affected approximately 4.9 million military clinic and hospital patients who were enrolled in TRICARE, the federal government's military healthcare provider (SAIC oversaw TRICARE's data security). The data had been stolen from an SAIC employee's car, and the victims included active and retired military personnel as well as their families. No financial data was involved, but sensitive information exposed included Social Security numbers, phone numbers, home addresses, and other personal data.

3. Excellus BlueCross BlueShield: 10+ Million Affected (September 2015)

In August 2015, Excellus discovered a cyber attack that had claimed the private information of approximately 10 million members. After a rash of cyber attacks targeting healthcare data in early 2015 (including the Premera and Anthem data breaches described below), Excellus ordered a forensic review of its own systems. They discovered it to be the third-largest healthcare data theft in history. The violation extended to as early as December 2013 and involved medical data, Social Security numbers, and financial information.

2. Premera Blue Cross: 11+ Million Affected (January 2015)

- In early 2015, Premera Blue Cross announced a cyberattack that had exposed the medical information of 11 million customers. Among other information, the attack had exposed bank account numbers, Social Security numbers, date of birth, and claims information. Premera's announcement of the second-largest healthcare infringe ever came just six weeks after the disclosure of the largest healthcare data breach ever.

1. Anthem Blue Cross: 78.8 Million Affected (January 2015)

January 2015 was a historically bad month for healthcare data. In the biggest healthcare breach to date (and, hopefully, ever), Anthem disclosed on January 29, 2015 that 78.8 million patient records had been stolen. The cyber attack claimed highly sensitive data that included names, Social Security numbers, home addresses, and dates of birth. The victims were largely Anthem health plan members and some were non-membersas Anthem also managed paperwork for several independent insurance companies.

References

[1]. Donaldson MS, Lohr KN. Health Data in the Information Age: Use, Disclosure, and Privacy. Washington, D.C.: National Academies Press, 1994.

[2]. Health Privacy Project. Health Privacy Stories, Available at: www.healthprivacy.org/newsletter-url2306/newsletter-url_show.htm?doc_id=34076. Accessed Jan 3, 2012.

[3]. Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure. For the Record: Protecting Electronic Health Information. Washington, DC: National Academies Press, 1997.

[4]. Lo B, Alpers A. Uses and abuses of prescription drug information in pharmacy benefits management programs. JAMA 2000; 283:801-6.

[5]. Beverly Kopala, PhD,RN, Mary Ellen Mitchell MA,RN, Use of Digital Health Records raises Ethics Concern, JONA's Healthcare Law , ethics, and Regulation, September 2011, Volume 13, Pages 84-89

[6]. Laymen , Elizabeth J, PhD, RHIA, CCS, FAHIMA Ethical issues and the electronic Health Record,

[7]. Anderson, Ross J. "A security policy model for clinical information systems." *Security and privacy, 1996. proceedings., 1996 ieee symposium on*. IEEE, 1996.

IOSR Journal of Business and Management (IOSR-JBM) is UGC approved Journal with Sl. No. 4481, Journal no. 46879.

Sakhi John. Electronic Medical Record For Deliverance of Effective Healthcare Delivery: Ethical Issues And Challenges of Digitalization In Clinical Information And Electronic Medical Records (EMR) Management." IOSR Journal of Business and Management (IOSR-JBM) 20.3 (2018): 01-06.